

使用REST API配置ISE訪客帳戶

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[在ISE上啟用ERS](#)

[為ERS設定管理員和保證人帳戶](#)

[建立訪客帳戶](#)

[讀取、更新、刪除訪客資料](#)

[驗證](#)

[疑難排解](#)

簡介

本文說明如何使用表示狀態傳輸(REST)API功能在身份服務引擎(ISE)上執行訪客相關任務。思科訪客API是一組基於REST的操作，提供安全的HTTPS和經過身份驗證的訪問來管理思科訪客使用者。藉助API，您可以建立、讀取、更新、刪除和搜尋訪客使用者。

必要條件

需求

思科建議您瞭解以下主題：

- ISE
- 外部RESTful服務
- 休息的客戶如失眠、休息等。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ISE版本2.6
- 失眠REST客戶端v7.1.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

附註：其他ISE版本的過程相似或相同。除非另有說明，否則您可以在所有2.x ISE軟體版本上使用這些步驟。

背景資訊

為了使用API，需要在ISE中設定啟用外部RESTful服務(ERS)和發起人身份驗證。ERS支援基本身份驗證，通過埠9060運行。身份驗證憑證已加密，並且是請求標頭的一部分。ERS要求ISE管理員為使用者分配特殊許可權以執行操作。

本文檔將介紹以下配置步驟：

- 1.在ISE上啟用ERS
- 2.為ERS設定管理員和發起人帳戶
- 3.建立訪客帳戶
- 4.讀取、更新、刪除訪客資料

設定

在ISE上啟用ERS

要在ISE上使用REST API功能，必須啟用ERS。

導覽至Administration > System > Settings > ERS settings > Enable ERS for read/write，如下圖所示。

ERS Settings

▼ General

External RESTful Services (ERS) is a REST API based on HTTPS over port 9060. The ERS service is disabled by default. An ISE Administrator with the "ERS-Admin" or "ERS-Operator" group assignment is required to use the API. For more information, please visit the ERS SDK page at: [https://\[redacted\]:9060/ers/sdk](https://[redacted]:9060/ers/sdk)

▼ ERS Setting for Administration Node

Enable ERS for Read/Write

Disable ERS

▼ CSRF Check

USE CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)

Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)

Save Reset

所有與ERS相關的資訊都在ISE的HTTPS埠9060上作為軟體開發套件(SDK)提供。啟用ERS並使用具有「ERS-Admin」或「ERS-Operator」許可權的管理員帳戶登入後，可以訪問此功能。

為ERS設定管理員和保證人帳戶

為了使用ERS，ISE需要具有為其分配的ERS-Admin或ERS-operator許可權的管理帳戶。需要建立管理員帳戶並將其新增到各自的組中。或者，ERS訪問也適用於超級管理員帳戶。

為了將API用於訪客功能，ERS管理員需要門戶的原始資料，如門戶ID、訪客身份組等。但是，為了讀取/建立/更新或刪除任何訪客資料，需要啟用ERS訪問許可權的發起人帳戶。

- 在本檔案中，使用內部ISE使用者帳戶作為發起人。
- 導覽至Administration > Identity Management > Identities，然後新增網路存取使用者，如下圖所示。

The screenshot shows the 'New Network Access User' configuration page. The 'Name' field is set to 'Sponsor_ERS' and the 'Status' is 'Enabled'. The 'Password Type' is 'Internal Users'. The 'Login Password' and 'Re-Enter Password' fields are masked with asterisks. The 'User Groups' dropdown menu is open, showing a list of groups: ALL_ACCOUNTS (default), Employee, GROUP_ACCOUNTS (default), GuestType_Contractor (default), GuestType_Daily (default), GuestType_SocialLogin (default), GuestType_Weekly (default), and OWN_ACCOUNTS (default). The 'Submit' and 'Cancel' buttons are at the bottom.

- 必須將此使用者帳戶新增到其中一個發起人組。
- 示例帳戶對映到名為ALL_ACCOUNTS的預設發起人組。
- 若要允許此發起組的ERS訪問，請轉到工作中心>訪客訪問>門戶和元件>發起人組，然後開啟分配的發起人組。
- 啟用選項：使用程式設計介面(Guest REST API)訪問思科ISE訪客帳戶，如圖所示。

Sponsor Can

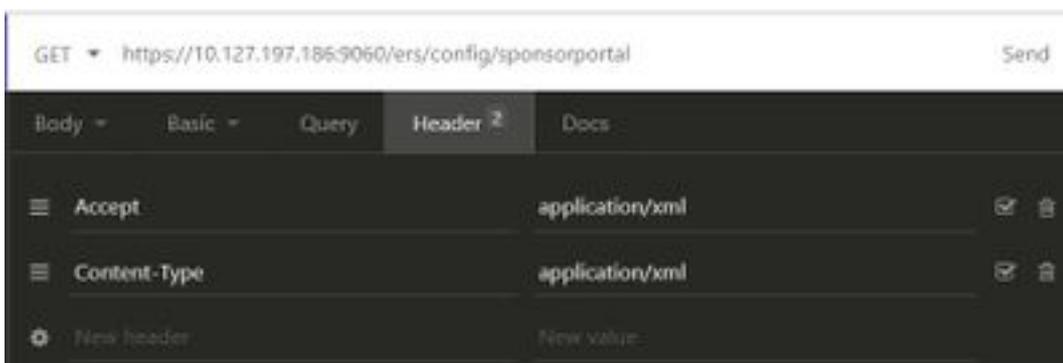
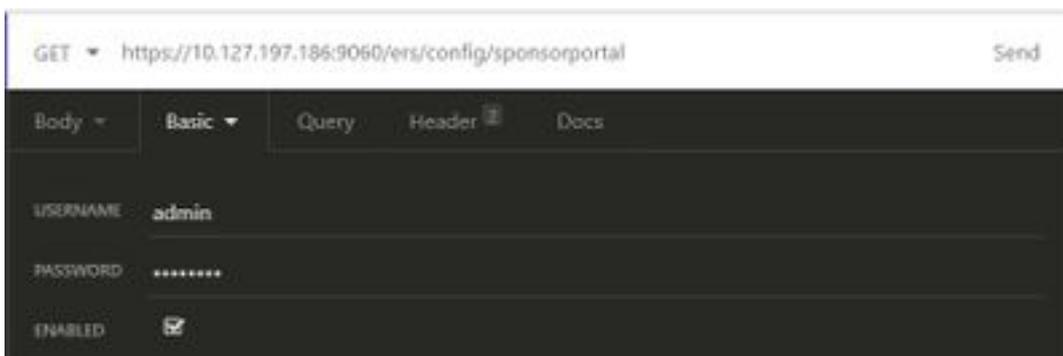
- Update guests' contact information (email, Phone Number)
- View/print guests' passwords
- Send SMS notifications with guests' credentials
- Reset guests' account passwords
- Extend guest accounts
- Delete guests' accounts
- Suspend guests' accounts
 - Require sponsor to provide a reason
- Reinstate suspended guests' accounts
- Approve and view requests from self-registering guests
 - Any pending accounts
 - Only pending accounts assigned to this sponsor ⓘ
- Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)

建立訪客帳戶

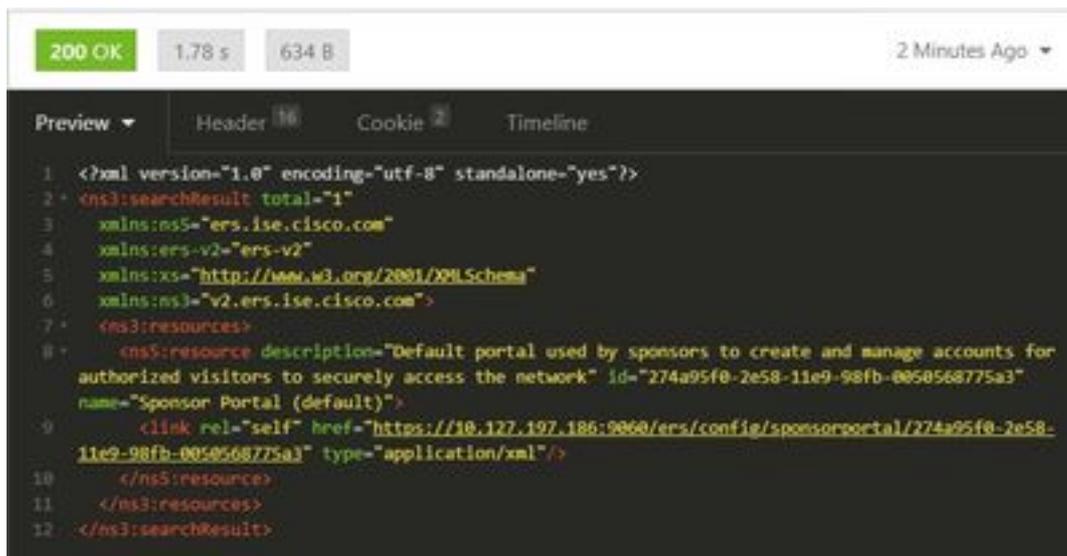
為了通過API建立訪客帳戶，必須將API呼叫作為發起人並通過其識別的發起門戶進行ISE。

步驟1。若要獲取在ISE上預配置的所有發起人門戶的門戶ID，請使用具有此處提供的資訊的任何REST客戶端：

方法	GET
URL	https://<ISE-IP>:9060/ers/config/sponsorportal
憑證	使用ERS管理員憑據
標頭	Content-Type:application/xml 接受:application/xml



預期輸出：



```
1 <?xml version="1.0" encoding="utf-8" standalone="yes"?>
2 <ns3:searchResult total="1"
3   xmlns:ns5="ers.ise.cisco.com"
4   xmlns:ers-v2="ers-v2"
5   xmlns:xs="http://www.w3.org/2001/XMLSchema"
6   xmlns:ns3="v2.ers.ise.cisco.com">
7 <ns3:resources>
8   <ns5:resource description="Default portal used by sponsors to create and manage accounts for
9     authorized visitors to securely access the network" id="274a95f0-2e58-11e9-98fb-0050568775a3"
10    name="Sponsor Portal (default)">
11     <link rel="self" href="https://10.127.197.186:9060/ers/config/sponsorportal/274a95f0-2e58-
12     11e9-98fb-0050568775a3" type="application/xml"/>
13   </ns5:resource>
14 </ns3:resources>
15 </ns3:searchResult>
```

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<ns3:searchResult total="1"
xmlns:ns5="ers.ise.cisco.com"
xmlns:ers-v2="ers-v2"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ns3="v2.ers.ise.cisco.com">
<ns3:resources>
<ns5:resource description="Default portal used by sponsors to create and manage accounts for
authorized visitors to securely access the network"
id="274a95f0-2e58-11e9-98fb-0050568775a3" name="Sponsor Portal (default)">
<link rel="self" href="https://10.127.197.186:9060/ers/config/sponsorportal/274a95f0-2e58-11e9-
98fb-0050568775a3" type="application/xml"/>
</ns5:resource>
</ns3:resources>
</ns3:searchResult>
```

感興趣的值是發起人門戶的門戶ID，用於建立訪客使用者。在本例中，ID是「274a95f0-2e58-11e9-98fb-0050568775a3」。

步驟2.使用此API呼叫建立訪客帳戶。這裡的portalID值是從步驟1取得的。

方法	POST
URL	https://<ISE-IP>:9060/ers/config/guestuser/
憑證	使用發起人帳戶憑據
標頭	Content-Type:application/vnd.com.cisco.ise.identity.guestuser.2.0+xml 接受:application/vnd.com.cisco.ise.identity.guestuser.2.0+xml
本文	<?xml version="1.0" encoding="UTF-8"?> <ns2:guestuser xmlns:ns2="identity.ers.ise.cisco.com"> <自定義欄位> </customFields> <訪客訪問資訊> <fromDate>04/25/2020 18:55</fromDate> <location>德里</location>

```
<toDate>04/28/2020 19:55</toDate>
<validDays>3</validDays>
</guestAccessInfo>
<來賓資訊>
<company>Cisco</company>
<emailAddress>abcd@cisco.com</emailAddress>
<firstName>John</firstName>
<lastName>Doe</lastName>
<notificationLanguage>英文
</notificationLanguage>
<password>9618</password>
<phoneNumber>9999998877</phoneNumber>
<smsServiceProvider>全域性預設值
</smsServiceProvider>
<userName>johndoe</userName>
</guestInfo>
<guestType>Contractor ( 預設 ) </guestType>
<personBeingVisited>abcd3@cisco.com</personBeingVisited>
<portalId>274a95f0-2e58-11e9-98fb-0050568775a3</portalId>
<reasonForVisit>從會計部訪問
Bob</reasonForVisit>
</ns2:guestuser>
```

附註：此處顯示的正文內容可用作模板（在SDK中也可用）。確保fromDate和toDate與validDays對應。位置、訪客型別和其他值在引用所使用的ISE時必須有效，只有這樣，呼叫才會成功。

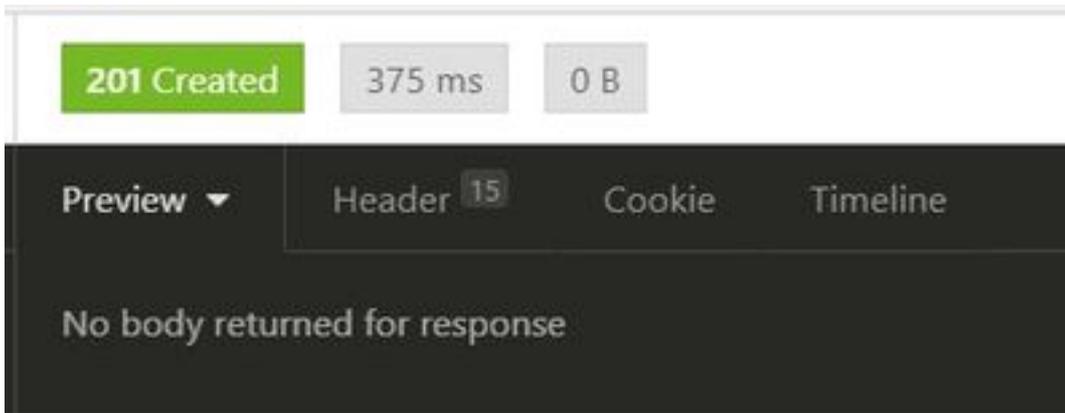
附註：進行此呼叫時使用的憑據必須是對映到發起人組的有效發起人帳戶。這裡的ERS管理員憑據無法正常工作。有關詳細資訊，請參閱本指南的前一節。

```
POST https://10.127.197.186:9060/ers/config/guestuser/ Send
XML Basic Query Header Docs
1 <?xml version="1.0" encoding="UTF-8"?>
2 <ns1:guestuser xmlns:ns1="identity.ers.ise.cisco.com">
3 <customFields>
4 </customFields>
5 <guestAccessInfo>
6 <fromDate>04/25/2020 18:55</fromDate>
7 <location>Delhi</location>
8 <toDate>04/28/2020 19:55</toDate>
9 <validDays>3</validDays>
10 </guestAccessInfo>
11 <guestInfo>
12 <company>Cisco</company>
13 <emailAddress>abc@cisco.com</emailAddress>
14 <firstName>John</firstName>
15 <lastName>Doe</lastName>
16 <notificationLanguage>English</notificationLanguage>
17 <password>9618</password>
18 <phoneNumber>9999990877</phoneNumber>
19 <serviceProvider>Global Default</serviceProvider>
20 <username>johndoe</username>
21 </guestInfo>
22 <guestType>Contractor (default)</guestType>
23 <personBeingVisited>abc3@cisco.com</personBeingVisited>
24 <portalId>274a95f8-2e58-11e9-98fb-0050568775a3</portalId>
25 <reasonForVisit>Netflix and chill</reasonForVisit>
26 </ns1:guestuser>
27
```

```
POST https://10.127.197.186:9060/ers/config/guestuser/ Send
XML Basic Query Header Docs
USERNAME Sponsor_ERS
PASSWORD *****
ENABLED 
```

```
POST https://10.127.197.186:9060/ers/config/guestuser/ Send
XML Basic Query Header Docs
Content-Type application/vnd.com.cisco.ise.identity.guestuser
Accept application/vnd.com.cisco.ise.identity.guestuser
New Header New value
```

預期輸出：



導航到ISE GUI > Master GuestReport，以驗證是否建立了帳戶：



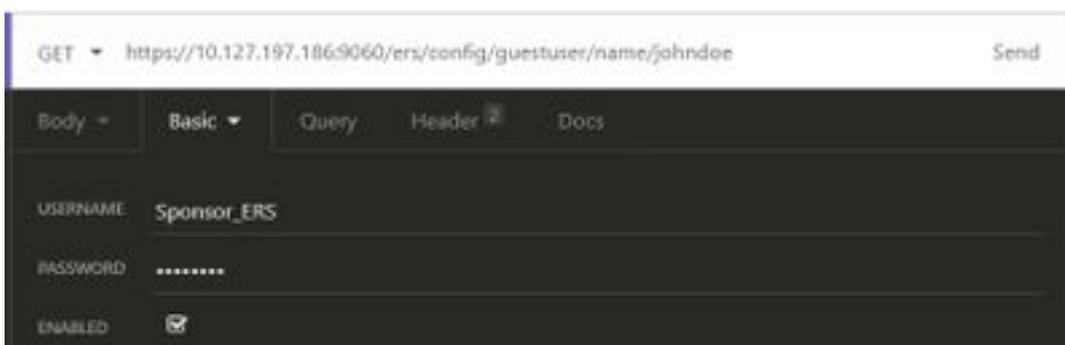
附註：無法從發起人門戶指定每個訪客帳戶的自定義使用者名稱和密碼組合。這個API方法可以用來滿足這個要求。

讀取、更新、刪除訪客資料

以下是一些對訪客資料執行各種操作的API呼叫示例。SDK中提供了所有可用的選項及其格式。

- 按名稱獲取訪客使用者帳戶詳細資訊：

方法 GET
 URL https://<ISE-
 IP>:9060/ers/config/guestuser/name/{name}
 憑證 使用發起人帳戶憑據
 標頭 Content-Type:application/xml
 接受:application/xml



預期輸出：

200 OK

```
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<ns4:guestuser id="3b967932-86f8-11ea-aafe-72889dc971d1" name="johndoe"
```

```
xmlns:ers="ers.ise.cisco.com"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ns4="identity.ers.ise.cisco.com">
<link rel="self" href="https://10.127.197.186:9060/ers/config/guestuser/name/johndoe"
type="application/xml"/>
<customFields/>
<guestAccessInfo>
<fromDate>04/25/2020 18:55</fromDate>
<location>Delhi</location>
<toDate>04/28/2020 19:55</toDate>
<validDays>3</validDays>
</guestAccessInfo>
<guestInfo>
<company>Cisco</company>
<creationTime>04/25/2020 18:55</creationTime>
<emailAddress>abcd@cisco.com</emailAddress>
<enabled>>false</enabled>
<firstName>John</firstName>
<lastName>Doe</lastName>
<notificationLanguage>English</notificationLanguage>
<password>9618</password>
<phoneNumber>9999998877</phoneNumber>
<smsServiceProvider>Global Default</smsServiceProvider>
<userName>johndoe</userName>
</guestInfo>
<guestType>Contractor (default)</guestType>
<personBeingVisited>abcd3@cisco.com</personBeingVisited>
<reasonForVisit>Visiting Bob from Accounting</reasonForVisit>
<sponsorUserId>1f7627f0-86f8-11ea-aafe-72889dc971d1</sponsorUserId>
<sponsorUserName>Sponsor_ERS</sponsorUserName>
<status>AWAITING_INITIAL_LOGIN</status>
</ns4:guestuser>
```

200 OK

422 ms

1244 B

3 Minutes Ago

Preview Header Cookie Timeline

```
1 <?xml version="1.0" encoding="utf-8" standalone="yes"?>
2 <ns4:guestuser id="3b967932-86f8-11ea-aafe-72889dc971d1" name="johndoe"
3   xmlns:ers="ers.ise.cisco.com"
4   xmlns:xs="http://www.w3.org/2001/XMLSchema"
5   xmlns:ns4="identity.ers.ise.cisco.com">
6   <link rel="self" href="https://10.127.197.186:9060/ers/config/guestuser/name/johndoe"
7   type="application/xml"/>
8   <customFields/>
9   <guestAccessInfo>
10    <fromDate>04/25/2020 18:55</fromDate>
11    <location>Delhi</location>
12    <toDate>04/28/2020 19:55</toDate>
13    <validDays>3</validDays>
14  </guestAccessInfo>
15  <guestInfo>
16    <company>Cisco</company>
17    <creationTime>04/25/2020 18:55</creationTime>
18    <emailAddress>abcd@cisco.com</emailAddress>
19    <enabled>>false</enabled>
20    <firstName>John</firstName>
21    <lastName>Doe</lastName>
22    <notificationLanguage>English</notificationLanguage>
23    <password>9618</password>
24    <phoneNumber>9999998877</phoneNumber>
25    <smsServiceProvider>Global Default</smsServiceProvider>
26    <userName>johndoe</userName>
27  </guestInfo>
28  <guestType>Contractor (default)</guestType>
29  <personBeingVisited>abcd3@cisco.com</personBeingVisited>
30  <reasonForVisit>Netflix and chill</reasonForVisit>
31  <sponsorUserId>1f7627f0-86f8-11ea-aafe-72889dc971d1</sponsorUserId>
32  <sponsorUserName>Sponsor_ERS</sponsorUserName>
33  <status>AWAITING_INITIAL_LOGIN</status>
34 </ns4:guestuser>
```

- 重置訪客使用者密碼：

這需要首先從呼叫獲取訪客ID，然後使用此API中的該ID。在此示例中，訪客ID為「3b967932-86f8-11ea-aafe-72889dc971d1」。

方法	PUT
URL	https://<ISE-IP>:9060/ers/config/guestuser/resetpassword/{id}
憑證	使用發起人帳戶憑據
標頭	Content-Type:application/xml 接受:application/xml

此方法不允許指定新密碼。ISE將使用新的自動生成的密碼返回輸出。

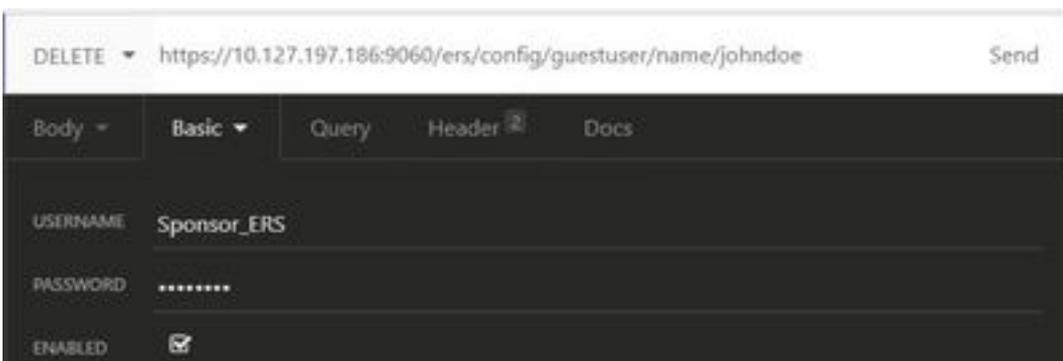
預期輸出：

```
200 OK

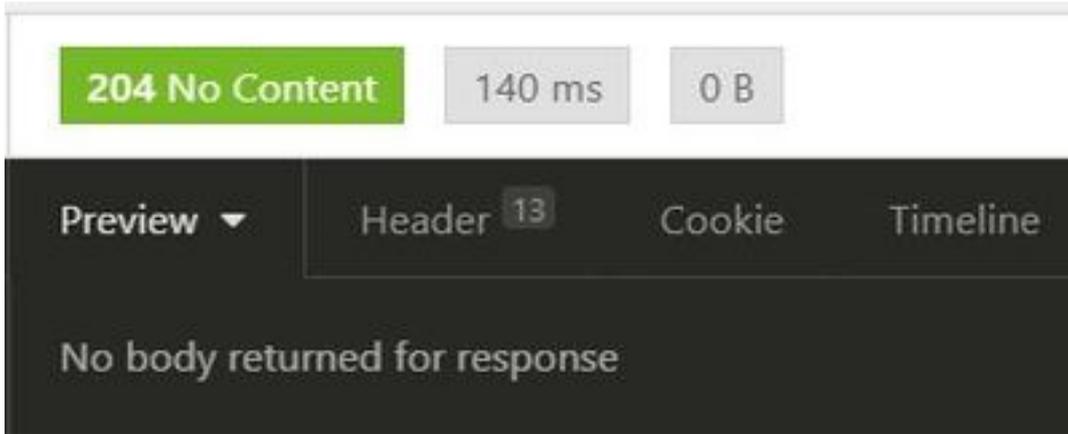
<?xml version="1.0" encoding="utf-8" standalone="yes"?>
<ns3:operationResult
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:ns3="ers.ise.cisco.com">
<attributesList>
<attribute name="password" value="2557" />
</attributesList>
</ns3:operationResult>
```

- 按名稱刪除訪客帳戶：

方法	刪除
URL	https://<ISE-IP>:9060/ers/config/guestuser/name/{name}
憑證	使用發起人帳戶憑據
標頭	Content-Type:application/xml 接受:application/xml



預期輸出：



驗證

目前沒有適用於此組態的驗證程序。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

一些常見錯誤及其可能的原因：

- 訪客帳戶建立失敗，錯誤為：

```
401 Unauthorized
```

```
<message type="ERROR" code="CRUD operation exception">  
<title>Sponsor does not have permission to access REST Apis</title>  
</message>
```

修正:這意味著用於使訪客帳戶的發起人帳戶對映到未啟用ERS訪問的發起人組。編輯與此對應的發起人組並使用程式設計介面(Guest REST API)啟用訪問思科ISE訪客帳戶。

```
400 Bad Request
```

```
<message type="ERROR" code="CRUD operation exception">  
<title>Creating GuestUser failed due to  
com.cisco.cpm.guestaccess.validation.GuestAccessValidationException: Portal not found for portal  
session e1fc15a7-a170-4d6a-b02c-0ab7b0bc54ff</title>
```

修正:在ISE上輸入的門戶ID不存在或不正確。從發起人門戶的「Get」呼叫獲取該門戶的正確門戶ID。

- API響應代碼及其可能的含義：
 - 200 (確定)：指示REST API成功執行了所需的操作。
 - 201 (建立)：表示在集合內建立了資源。
 - 204 (無內容)：這通常作為對PUT、POST或DELETE請求的響應傳送。

400 (錯誤請求) : 用於請求語法格式錯誤、引數無效等問題的通用錯誤代碼。閱讀消息詳細資訊 (如果可用) 以瞭解原因。

401 (未授權) : 這表示執行操作所使用的憑據錯誤、沒有憑據或帳戶無權執行此操作。

500 (內部伺服器錯誤) : 指示伺服器端的問題。登入ISE可幫助瞭解原因。

有關ISE的REST API用法的詳細資訊，請參閱[Guest REST API](#)。